

第1章 機能によって安全を確保する「機能安全」の考え方を知る

田辺安雄

組み込みシステム設計者のためのIEC 61508解説

ここでは，「機能安全」という考え方について解説する．また，組み込みシステムなどによって機能安全を確保するための国際規格「IEC 61508」について解説する．本規格は欧州などの産業界において強制規格に近いものとしてとらえられており，組み込みシステム技術者にとって無視できない存在となりつつある．（編集部）

1．組み込みシステムのための安全規格，IEC 61508

2006年は，街中にあるエレベータや身近な家庭用品の安全にかかわる問題がメディアに取り上げられ，一般の方々も安全や安心といった問題に対して深い関心を寄せた年だと言えるでしょう．事故があると，安全にかかわる問題への関心が高まります．また，その都度，批判がなされ，対策が講じられ，経営者が深々と謝罪の言葉を述べるといった構図が繰り返されています．「対応が後手になっている」という印象を多くの方が共通して持っていることと思います．

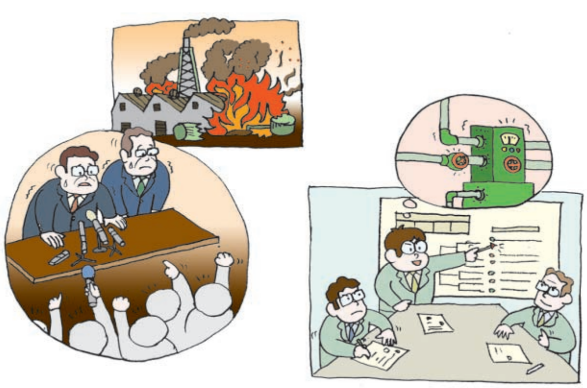


図1　事後対策から事前対策へ

海外では，1976年のイタリアSevesoにおける化学工場からのダイオキシン飛散事故，1979年の米国ペンシルバニア州Three Mile Island原子力発電所事故，1984年のインドBhopalにおける農薬工場からの有毒ガス流出，1986年のウクライナChernobyl原子力発電所事故など，それまでに経験したことのない大きな事故がありました．これらの事故をきっかけに，欧州や米国では，発生した事故に対する事後対策よりも，潜在危険（hazard）をあらかじめ徹底的に分析してリスクを評価し，事前に対策を講じるという安全確保の考え方に次第に移行するようになりました（図1）．

他方では，さまざまな産業の安全確保の目的で，コンピュータ技術が盛んに使用されるようになってきました．

このような，新たな考え方や技術の出現に対して，国際電気標準会議（International Electrotechnical Commission：IEC）は2000年に，コンピュータ技術による機能安全を確保するための国際規格「IEC 61508[(1)]（国内における翻訳規格はJIS C 0508[(2)]）」を発行しました．

IEC 61508は任意規格であり，規格そのものには法的な拘束力はありません．しかし，海外の産業界では，強制規格に近いとらえ方をしています．これは，システムや組織をIEC 61508に適合させることで企業責任を果たし，これによって国際競争力を高める意図があります．

2000年から2005年にかけてIECは，原子力やプロセス産業，鉄道，産業機械などの各分野における機能安全規格

KeyWord　機能安全，IEC 61508，JIS C 0508，潜在危険，hazard，リスク，危害，安全関連系，SIL，HAZOP，FTA，ETA，目標機能失敗尺度，安全ライフ・サイクル，多重化，冗長化，PL法

(IEC 61508のサブ規格)を制定しました．さらに，国際標準化機構(International Organization for Standardization：ISO)が自動車分野における機能安全規格を現在審議中であり，2008年に制定する予定となっています．このようにして，多くの産業分野に機能安全の考え方が浸透してきており，各国で関心が急速に高まっています．

IEC 61508の規格書は400ページもあり，難解という指摘もあります．ここでは，機能安全規格の基本的な考え方について，分かりやすく解説します．

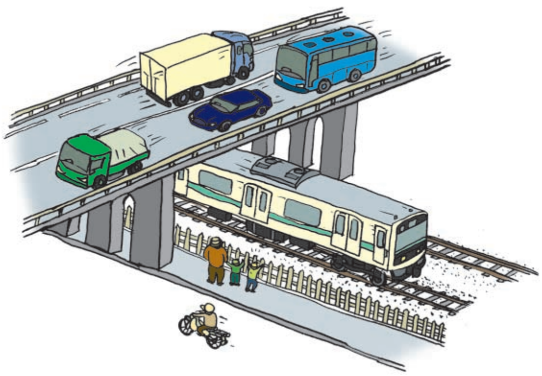


図2　立体交差にすれば踏切事故はなくなる(本質安全)

● 次善の策としての機能安全

機能安全は，「本質安全」という考え方に対比される新しい概念です．例として鉄道を考えてみましょう．踏切事故をなくすためには，立体交差にするのが最も確実な方法です(図2)．このような対策によって根源からリスクをなくして達成する安全のことを，本質安全と呼びます．

しかし現実的には，すべての踏切を立体交差にはできません．このため，信号や列車停止装置などの周辺の安全機能によって相対的にリスクを軽減させ，リスクを許容できる程度以下にします．このような対策によって安全を確保することを機能安全と呼びます．もちろん，本質安全を達成できた方が良いのは言うまでもありません．

ここで言うリスクとは，「危害の発生頻度と危害の過酷さの組み合わせ」を指しています(3)．機能安全規格であるIEC 61508は，システムにどのような危険が潜んでいてどのような頻度で発生するのか，また，それが発生した場合の危害(harm)のひどさはどの程度なのかを想定し，リスクを許容できる範囲内に収めるための管理の枠組みを規定しています(用語の定義については，下掲のコラム「危害・潜在危険・リスク」を参照のこと)．

● 安全関連系の故障も視野に入れる

リスクを軽減するために設置するシステムを「安全関連系(safety related system)」と呼びます．機構による技術や防護壁などの設備も安全関連系に含まれますが，IEC 61508は電気的な原理で動作する機器やシステムを対象としています．例えば，PLC(programmable logic controller)やマイコン，プロセッサ，メモリ，LSI(large scale integrated circuit)，ASIC(application specific integrated circuit)，センサ，トランスミッタ，アクチュエータなどが対象となります．

具体的なシステムとしては，自動車分野におけるECU(electronic control unit)，化学プラント分野における安全計装システム(safety instrumented system：SIS)，原子力分野におけるC&I(Control & Instrumentation)，産業機械分野におけるSRECS(safety related electronic control system)などが該当します．IEC 61508ではこれらを総称して，「電気・電子・プログラマブル電子(Electrical/Electronic/Programmable Electronic)」の安全関連系と呼んでいます．

一般に，ハードウェア(コンピュータの部品など)は故障

COLUMN 危害・潜在危険・リスク

本稿では，危害と潜在危険，リスクを以下のように使い分けています．

- 危害(harm)：身体への障害や健康状態の悪化などを指す
- 潜在危険(hazard)：危害に至る影響の源を指す．潜在しているだけなら危害には至らない．人為ミスや装置の故障などによって顕在化した場合に危害となって現れる
- リスク：危害の発生頻度と危害の過酷さを組み合わせたもの

hazardについては，危険源，危険因子などとも訳されます．例えば，機械類を安全に設計するための国際規格「ISO 12100(翻訳規格JIS B 9700)」においては，hazardを「危険源」と訳しています．それに対し，IEC 61508(翻訳規格JIS C 0508)においては，危険の原因となる要素が見えやすい機械類と比べて，「システムのどこに潜んでいるのか分からない危険」というニュアンスを含んだ訳語として「潜在危険」を当てたそうです．

します．また，ソフトウェアには不具合（バグなどのソフトウェア・エラー）があります．安全関連系が作動するべき事態になったとき，それが不具合によって動作しなければ事故に至る可能性があります．安全の確保は，安全関連系にかかわるさまざまな企業に広く関係する問題であり，システムの設計や運用，保守などを担当する企業を網羅する仕組みが必要です．このため，IEC 61508は，製品の概念から設計，保守，改修，廃却に至るまでの製品のライフ・サイクル全体を通して，業務プロセスを定義しています（**図3**）．

IEC 61508（JIS C 0508）は以下の7部によって構成されています．機能安全の概要を知るには，**図3**に示した管理業務の全体像や潜在危険，リスク解析，安全度水準（safety integrity level：SIL）などについて規定している第1部を読むことをお勧めします．

- 第1部：一般要求事項
- 第2部：電気・電子・プログラマブル電子安全関連系に対する要求事項
- 第3部：ソフトウェア要求事項
- 第4部：用語の定義および略語
- 第5部：安全度水準（SIL）決定方法の事例
- 第6部：第2部および第3部の適用指針
- 第7部：技術および手法の概観

2．安全機能と安全度水準（SIL）を定義する

機能安全を確保するための重要な業務の一つに，安全関連系に対する安全要求事項の仕様作成があります（**図3**のフェーズ4に相当）．安全要求事項は，「安全機能」と「安全度水準（SIL）」から構成されます（**図4**）．安全機能とは，例えば，車が衝突したときに運転者を守るためにエア・バッグを作動させるといった，安全を確保するための機能です．SILとは，安全機能を作動させる事態になったときに，その機能（エア・バッグ）がどの程度の信頼性で作動する必要があるかを示す指標です．

以下に，安全機能や安全度水準を決めていく手順について説明します．

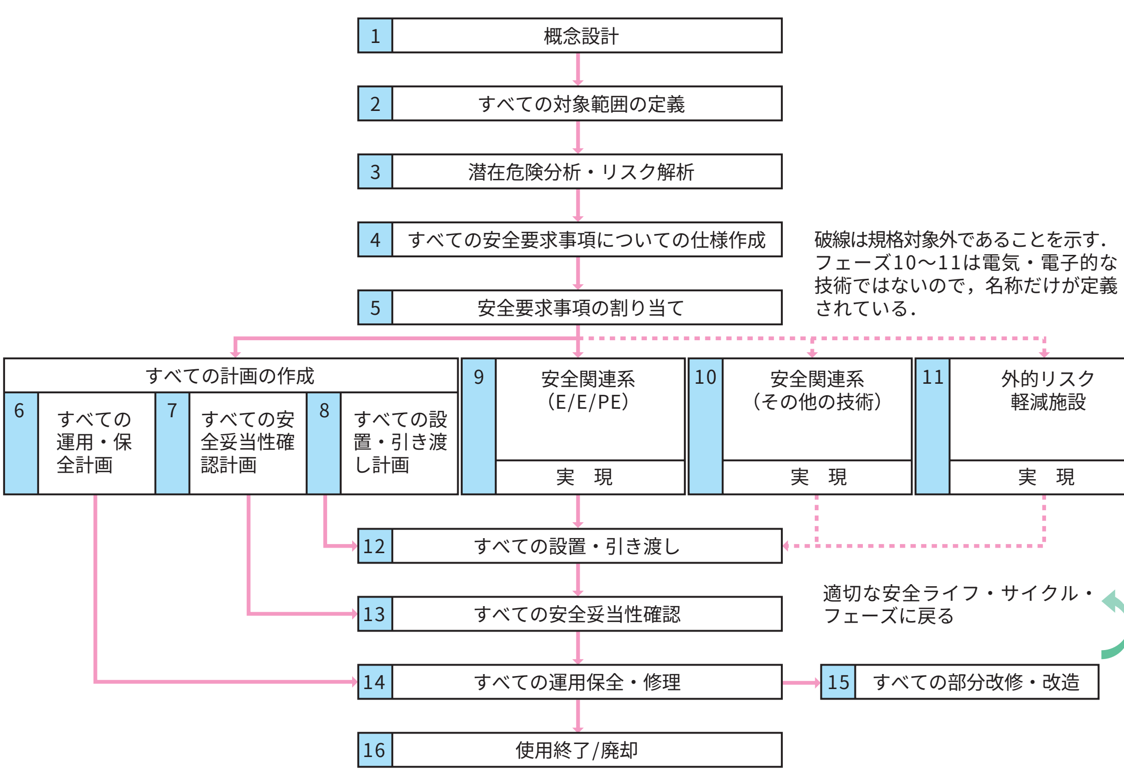


図3　システムのライフ・サイクル全般にわたる機能安全の管理業務

IEC 61508に採用された，電気・電子・プログラマブル電子（E/E/PE）の安全関連系に関するライフ・サイクル業務を16フェーズに分類・定義した概念図．「全安全ライフ・サイクル（overall safety life cycle）」とも呼ばれる．IEC 61508では，ゆりかごから墓場までの機能安全管理に関する業務を規定している．なお，図中の「すべての」とは「システム全体に対する」という意味である．

● 潜在危険を分析して安全機能を決定する

システムに必要な安全機能を決めるためには，システムにどのような潜在危険があるのかを分析します．潜在危険を分析する手法の一つとして，HAZOP（Hazard and Operability）スタディー[(4)]があります．これは，化学プラント用に開発された手法ですが，交通システムやコンピュータ・システムなどの分析にも使用されている汎用的な手法です．

HAZOPスタディーでは，システムの設計パラメータ（例えば，化学プラントのある反応容器周辺における「流量」や「温度」，「圧力」など）に対し，「なし（No）」，「過大（More）」，「過小（Less）」，「一部（Part of）」，「逆（Reverse）」などといったガイドワード（基準となる用語）を組み合わせて，安全上の特性を系統的に分析します（表1）．

分析に際しては，システム設計者や安全技術者，オペレータなどが議論を行います．あるシステム内の場所において，例えば，流量が過大（More）になった場合に，その原因と影響を同時に分析します．システム内のそれぞれの場所において，必要な対策を提案しながらHAZOPスタディーを進めていきます．その結果，要求される安全機能が決定されます．

● リスクが許容範囲内に収まるようにSILを決定する

次に，システムにおけるリスクを解析し，求めたリスクが許容できる範囲に収まるように，安全機能に要求される安全度水準（SIL）を決定します．この作業を「SILの割り当て」と呼びます（図3のフェーズ5に相当）．SILを割り当てるためには，許容できるリスクの範囲（許容リスク）を事前に決定しておく必要があります．

リスクを解析する手法としては，フォールト・ツリー解析（fault tree analysis：FTA）やイベント・ツリー解析（event tree analysis：ETA）による定量的な手法と，リスク・グラフやリスク・マトリックスなどの定性的な手法があります．

それぞれの安全度水準（SIL）に対して定められた数値目標を表2に示します．SILが高い（最高はSIL4）ほど，リスクは軽減されます．作動する頻度が低い安全関連系の場合（自動車のエア・バッグなど）と，頻度が高い安全関連系の場合（自動車のブレーキなど）では，数値目標が異なります．

それではここで，化学プラントの反応容器（図5）を例に，機能安全をどのようにして達成するのかを説明します．図中に示した「基本プロセス制御系」は，内部の液位を監視するセンサと，物質の流入を制御する制御弁から構成されています．「安全関連系」は，圧力を監視するセンサと，マイ

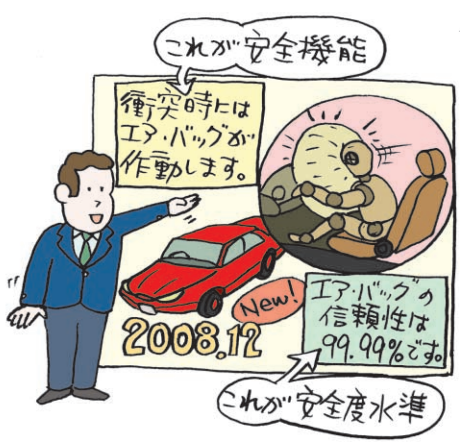


図4　安全要求事項＝安全機能＋安全度水準

表2　それぞれの安全度水準（SIL）に対して割り当てられた目標機能失敗尺度

作動要求の頻度により，割り当てられる目標機能失敗尺度の数値と単位が異なる．

SIL	低頻度作動要求モード運用（作動要求当たりの設計上の機能失敗平均確率）	高頻度作動要求または連続モード運用（単位時間当たりの危険側故障確率［1/時間］）
4	10^{-5}以上10^{-4}未満	10^{-9}以上10^{-8}未満
3	10^{-4}以上10^{-3}未満	10^{-8}以上10^{-7}未満
2	10^{-3}以上10^{-2}未満	10^{-7}以上10^{-6}未満
1	10^{-2}以上10^{-1}未満	10^{-6}以上10^{-5}未満

表1　HAZOPスタディーにおける分析例

各パラメータに対してさまざまなガイドワードを組み合わせて，潜在危険や対策を洗い出していく．

No	項目	機能・目的	パラメータ	ガイドワード	結果	原因	潜在危険	推奨事項	備考
1	配管	反応容器への移送	流量	No	流量損失，システム故障，機器損傷	配管漏えい：配管破断	機器損傷	―	―
2	配管	反応容器への移送	流量	More	圧力高，配管破断	圧力逃がし弁未設置	機器損傷	圧力逃がし弁装置，遮断弁設置	―
3	配管	反応容器への移送	流量	Less	反応物質低減	配管漏えい：配管破断	機器損傷	―	―

コンなどを使った遮断弁や逃がし弁から構成されています．逃がし弁は，機構的に弁を開放する，そのほかの技術による安全関連系です．

最初に，リスク目標を定義する必要があります．ここでは定量的な例として，「反応容器からガスが放出される頻度が，1年のうちに10^{-3}を超えないこと（1000年に1回以下）」という目標を考えます．

次に，イベント・ツリー解析（ETA）でリスクを計算してみます（**図6**）．このシステムにおいては，過度に圧力が上昇する事象が10年に1回発生すると想定します．警報（高圧アラーム）の作動および運転員の対応，逃がし安全弁の作動失敗確率をそれぞれ0.1とします．

ここで，遮断弁として，機能失敗平均確率が10^{-3}から10^{-2}の範囲にある（2けた以上のリスク軽減を図れる）SIL2のシステムを設置してみます．この遮断弁は，センサで圧力異常を検知した場合に，逃がし弁が作動する前に物質の流入を遮断します．これにより，放出頻度は1年に1.9×10^{-4}となり，目標値を満足します．従って，安全関連系である遮断弁のシステムにはSIL2を割り当てればよいことになります．

ここでは，リスクを定量的に割り当てる方法について紹介しましたが，定性的な方法も認められています[注1]．また，ほかの産業システムでも基本的な考え方は同じなので，身近なシステムに置き換えて考えてみてください．

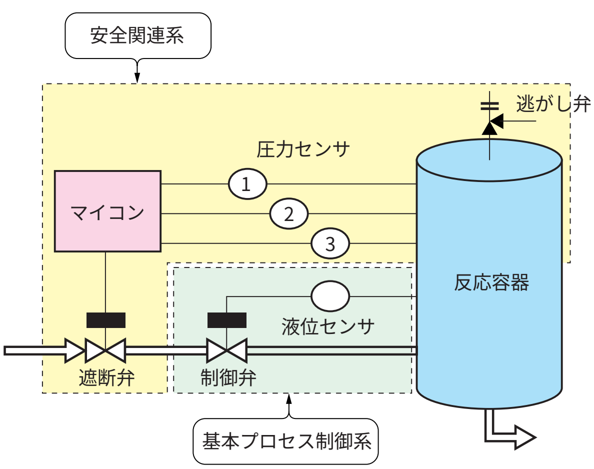


図5　安全関連系を有する化学反応容器
化学プラントの典型的な反応容器の例．3重化したセンサからの信号を論理回路（マイコンなど）で処理して，緊急時に遮断弁を閉止する．

3．機能安全を実現する

安全にかかわる故障は，ランダム・ハードウェア故障（確率論的原因故障）と決定論的原因故障に分類されます．

ランダム・ハードウェア故障は，ハードウェアに関して，部品や材料の劣化などによって起こる故障です．いつ発生するかは分かりませんが，発生頻度は定量化できます．

一方，決定論的原因故障は，発生してみて初めて分かるたぐいの故障であり，ハードウェアとソフトウェアの両方に関して発生します．ハードウェアに関しては，システムの設置前や設置中に，部品の組み合わせなどによって故障が起こり得ます．ソフトウェアに関しては，仕様の誤りやバグなどのソフトウェア故障が起こり得ます．一方，システムを設置した後には，誤使用という故障要因も考えられます．

● ランダム・ハードウェア故障には多重化で対策

ランダム・ハードウェア故障の対策としては，故障を検

注1：リスクを定量的に割り当てる方法とは，ここで述べたように，被害の大きさと頻度からリスクを割り出して，許容できるリスクよりも小さくなるようにSILを決定する方法である．リスクを定性的に割り当てる方法とは，被害の大きさと頻度，回避の可否，事象の発現回数などから，対応するべきSILを割り出す方法である．

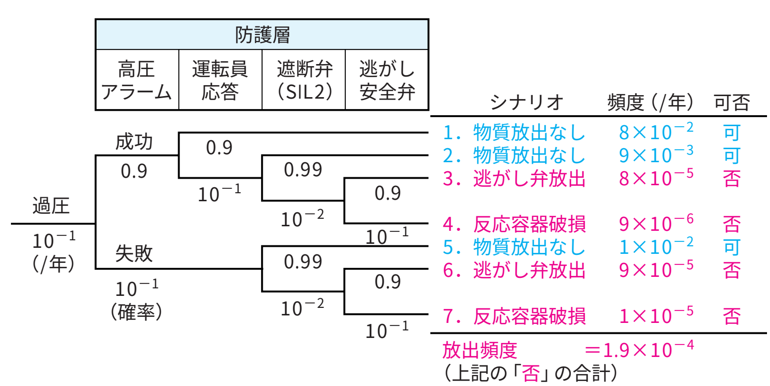


図6
イベント・ツリー解析
何らかの原因により，反応容器の内部のガスが外部に放出されるというシナリオを分析して，個別のシナリオの頻度を計算したイベント・ツリー図．過圧に至る事象は10年に1回発生すると仮定し，対応操作の成功確率/失敗確率を分岐上に示している．



図7 冗長ハードウェア構成の例

故障時の信頼性を向上させるために二重化したシステムの模式図．一方のチャネルにおいて故障が発生し，安全機能の達成ができなかったとしても，もう一方のチャネルで安全機能を実行できる．

表3 ソフトウェア・モジュール・テストと統合テストの技法

この技法の使い分けは，ソフトウェアのライフ・サイクル業務のフェーズ9.3で規定されている．

技術/手法	SIL1	SIL2	SIL3	SIL4
確率的テスト	―	推奨	推奨	強く推奨
動的分析・テスト	推奨	強く推奨	強く推奨	強く推奨
データ記録・分析	強く推奨	強く推奨	強く推奨	強く推奨
機能テスト・ブラックボックス・テスト	強く推奨	強く推奨	強く推奨	強く推奨
性能テスト	推奨	推奨	強く推奨	強く推奨
インターフェース・テスト	推奨	推奨	強く推奨	強く推奨

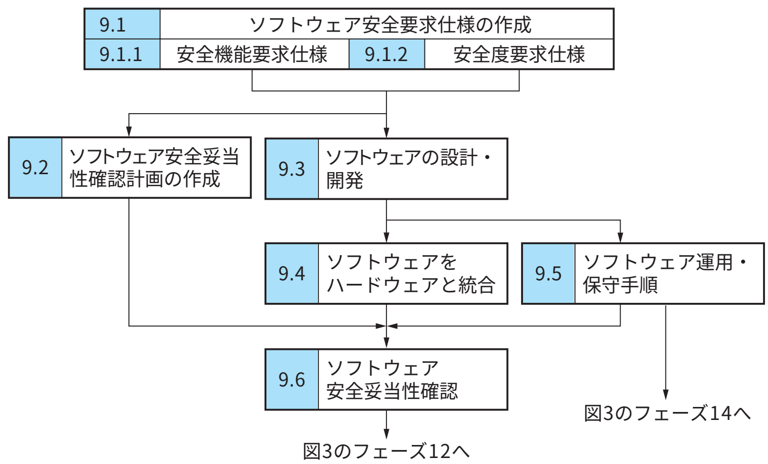


図8
ソフトウェアのライフ・サイクル業務

ライフ・サイクル全般にわたる機能安全の管理業務（図3）のフェーズ9は，ハードウェア・ライフ・サイクルとソフトウェア・ライフ・サイクルから構成される．このうちのソフトウェア・ライフ・サイクルを図示した．

知（診断）し，故障を隠す（多重化/冗長化）技術などが採用されます．

故障検知については，IEC 61508第2部の付属書Aに，CPUやバスなどの故障診断技術がまとめられています．

ハードウェアに対して要求される安全度水準（SIL）が高ければ高いほど，単一チャネルのハードウェア構成でそれを実現するのは難しくなります．そのため，ハードウェア構成を多重化して，一方のチャネルが故障により安全機能を喪失した場合はもう一方のチャネルによって安全機能を実行できるように設計します（図7）．

● 決定論的原因故障にはプロセス定義で対策

決定論的原因故障に対しては，ランダム・ハードウェア故障の対策はほとんど役に立たないと言われています．ハードウェアやソフトウェアを実装するにあたり，決定論的原因故障の対策としては，それぞれの業務プロセスを定義したライフ・サイクルに従って業務を実施することが求められます．各フェーズにおいて，割り当てられたSILに応じた技法を選択して業務を実施し，その結果を文書（ドキュメント）にまとめ，情報として次のフェーズに引き渡します．

例として，ソフトウェアのライフ・サイクルに対して定義されている業務プロセスを図8に示します．図中のフェーズ9.3では，ソフトウェアのアーキテクチャやシステム，モジュールといった，構造的なレベルにおける設計・開発に対する要求事項が規定されています．例えば，ソフトウェア・モジュールを対象にしたテストでは，ソフトウェアの安全要求事項を（要求される安全機能と安全度の両方の観点から）確かめることで，それぞれのソフトウェア・モジュールがその意図した機能を実行し，意図しない機能は実行しないことを明示する必要があります．このため，このフェーズには，フェーズ9.1からソフトウェア・モジュールのテスト仕様やソース・コードなどが引き継がれ，また次のフェーズ（フェーズ9.4とフェーズ9.5）には，ソフトウェア・モジュールのテスト結果とテスト済みのソフトウェア・モジュールが引き継がれていきます．

フェーズ9.3では，表3に示す六つのソフトウェア・モジュール・テストや統合テストの技法を，SILに応じて使い分けることが要求されています．

● 物差しとしてIEC 61508を活用する

機能安全はコンピュータ技術の普及と密接に関係して登場した，新しい安全確保の枠組みです．一方，事故やトラブルが発生した場合，製造物責任法（PL法）との関係が論じられることがあります．PL法は，製造物の欠陥による損害に対する賠償責任を規定した法律であり，国内では1994年に施行されました．PL法によると，損害が予見可能だったとみなされると，賠償責任を問われる可能性があるので，機能安全の考え方やIEC 61508とは非常に微妙な関係にあると言えます．

IEC 61508は，絶対安全はないという前提の規格ですから，この規格に従えば，「事故やトラブルが絶対になくなる」ということはあり得ません．しかし，IEC 61508は，さまざまな産業システムの安全性や，企業の安全の取り組みを比較できるように，世界の安全の専門家が長年かかって作成した安全の物差しです．普段の企業活動をIEC 61508に照らし合わせることにより，何が足りていて何が足りないのかを把握できます．また，発生した事故を，IEC 61508に照らして分析し，事故の教訓を体系的な枠組みの中で生かすこともできるでしょう．そうしていくことで，IEC 61508の本来の意図である「安心・安全な社会を実現・維持すること」が可能になると考えます．

IEC 61508は2008年に改訂される予定であり，現在，国際委員会で審議中です．新技術として，セキュリティ，オブジェクト指向モデリングなどについて，機能安全でどのように考えるべきかを審議しています．なお，今回の審議で改訂が終わりというわけではありません．コンピュータ技術の進歩に追従するべく，今後も改訂を重ねていくと思われます．

参考・引用＊文献

(1) IEC 61508, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems", Part1,2,4,5, 1998, Part2, 6, 7, 2000.
(2) JIS C 0508，「電気・電子・プログラマブル電子安全関連系の機能安全」，日本規格協会，第1，4，5部，1999年，第2，3，6，7部，2000年．
(3) ISO/IEC GUIDE 51:1999, "Safety aspects -- Guidelines for their inclusion in standards", Second edition, 1999.
(4) F. Redmill, M. Chudleigh, J. Catmur ; System Safety: HAZOP and Software HAZOP, John Wiley & Sons, 1999.

たなべ・やすお
(株)日本機能安全

<筆者プロフィール>
田辺安雄．1949年3月13日生まれ．大阪大学大学院工学研究科にて応用物理を専攻し，1974年4月，東芝に入社．原子力事業部にて原子炉の炉心設計，燃料設計および原子力プラントの遮へい設計，安全設計に従事．2001年11月から電力システム社の事業開発推進室にてIEC 61508やリスク評価の普及活動に従事．2005年3月，東芝を退職し，4月から関連会社であるアイテル技術サービスに入社，同業務を継続する，2005年10月，ガイア・システム・ソリューション入社，機能安全コンサルティング業務に従事．2006年7月，日本機能安全にて同業務に従事，現在に至る．IEC 61508国際委員会エキスパート，国内対策委員会委員．